REMARKS/ARGUMENTS

In the Office Action, the Examiner noted that claims 1-29 are pending in the application. The Examiner additionally stated that claims 1-29 are rejected. By this communication, claims 1, 4, 8, 10, 17, 20, 24, 27, and 29 are amended. Hence, claims 1-29 are pending in the application.

Applicant hereby requests further examination and reconsideration of the application, in view of the foregoing amendments.

In the Specification

Applicant has amended the specification to secure a substantial correspondence between the claims amended herein and the remainder of the specification. No new matter is presented.

In the Claims

Rejections Under 35 U.S.C. §103(a)

The Examiner rejected claims 1-29 under 35 U.S.C. 103(a) as being unpatentable over Qi, EP1215842 (hereinafter, "Qi"), Ulmann, "Designing a NICE Processor," Microprocessors and Microsystems, IPC Business Press LTD. London, GB, Vol. 23, No. 5. 25 October 1999. Pages 257-264 XP004321479 ISSN: 0141-9331 (hereinafter, "Ulmann"), and Lynch, US Patent 5828873 (hereinafter, "Lynch").. Applicant respectfully traverses the Examiner's rejections.

Regarding claim 1, the Examiner noted that Qi teaches "An apparatus for performing cryptographic operations, comprising: a cryptographic instruction, received by a [ ] as part of an instruction flow executing on said [ ], wherein said cryptographic instruction prescribes one of the cryptographic operations . . . text . . . (abstract: i.e., cryptographic processing, e.g., two level multiplexer)."

The Examiner conceded that Qi is not explicit about other features of claim 1.

The Examiner did noted that Ulmann teaches "computing device (section 1: i.e., processor)" for the motivation of escaping the typical flaws and drawbacks of other processors (section 1) and, thus, Ulmann teaches to make a processor that can handle

simplified operations such as described in Qi (the other reference). The Examiner stated that the hardware implementation, as broadly noted at abstract and detailed at other sections of Ulmann, is also noted.

The Examiner stated that Ulmann and Qi are not explicit about the other features of claim 1, but that Lynch teaches "translation logic; operatively coupled to said [ ] instruction, configured to translate said [ ] instruction into micro instructions, wherein said micro instructions are ordered to direct said computing device to load a second input [ ] block . . and to execute said one of the [ ] operations on said second input [ ] block prior to directing said [ ] to store an output [ ] block corresponding to a first input [.] block; whereby said output [ ] block is stored during execution of said one of the [ ] operations on said second input [ ] block (column 3, line 52 to column 4, line 17; figure 3, load/store unit 26; i.e., the loading and storing processes used when using load/store unit 26)" for the motivation of executing more without slowing down the processor (column 2, lines 21-37). The Examiner stated that, as noted by Applicant in the specification of this application (such as at pages 1-19), much of the concepts of the floating point processing (as detailed in Lynch) are readily applicable to the cryptography processing (as recited in the claim).

The Examiner thus concluded that it would have been obvious to those of ordinary skill in the art at the time of the claimed invention to combine the respective teachings of Qi, Ulmann, and Lynch for the motivation noted in the previous paragraphs so as to teach the claimed invention.

Applicant respectfully disagrees with the Examiner's characterization of the teachings of Qi, Ulmann, and Lynch, in view of that subject matter which is recited in claim 1, and offers the following points in traversal of the rejection.

Claim 1, as amended herein, is repeated below for ease of reference.

1. An apparatus for performing cryptographic operations, comprising:

a cryptographic instruction, received by fetch logic in a microprocessor as part of an instruction flow executing on said microprocessor, wherein said cryptographic instruction is retrieved from memory and prescribes one of the cryptographic operations;

translation logic, operatively coupled to said cryptographic instruction, configured to translate said cryptographic instruction into micro instructions, wherein said micro instructions are ordered to direct said microprocessor to load a second input text block from said memory and to execute said one of the cryptographic operations on said second input text block prior to directing said computing device to store an output text block corresponding to a first input text block to said memory;

whereby said output text block is stored during execution of said one of the cryptographic operations on said second input text block.

First, Qi does not teach a cryptographic instruction that is received by fetch logic in a microprocessor as part of an instruction flow executing on said microprocessor. Qi does not teach an instruction at all. Rather, Qi teaches a cryptography engine that can be decoupled from surrounding logic by using asynchronous buffers. (Abstract) Qi's hardware is algorithm and function specific and does not allow for specification of a cryptographic operation by a cryptographic instruction. In fact, the technique disclosed by Qi is indeed typical of those mechanisms which the present inventors have observed to be limiting because they must be fed by a CPU over a bus. Qi's object is to overcome a problem noted with hardware-based cryptographic accelerators, that is, latency due to asynchronous communications. Qi solves this problem through the use of pipelining and input/output FIFOs 401, 441 (see FIGURE 4 and related discussion).

Applicant's invention, in contrast, employs a cryptographic instruction that is received by a microprocessor (i.e., CPU) itself, as part of an instruction flow executing on the microprocessor. That is, the instruction can be embedded within an application program executing on the microprocessor. Applicant has searched Qi and finds that Qi utterly fails to teach, disclose, or suggest, a cryptographic instruction received by fetch logic in a

microprocessor as part of an instruction flow executing on said microprocessor, wherein said cryptographic instruction is retrieved from memory and prescribes one of the cryptographic operations.

Second, although Ulmann refers to a "processor," Applicant respectfully notes that 1) the execution of block cryptographic operations is not "simplified" as the Examiner asserts, and 2) Ulmann's stated purpose is more a basic tutorial on how to implement a processor using FPGAs that provides for conditional execution, a strict instruction set, and powerful addressing modes, along with a general purpose register set that is easily programmable and suite for educational purposes. Applicant asserts that prior to the present invention, no techniques existed to date that provided for incorporation of a cryptographic unit into a general purpose microprocessor, such as an x86-compatible microprocessor. This is because, as is noted in the instant disclosure, cryptographic processing is complicated and involves iterative execution (i.e., "rounds") on a plurality of input data blocks. Ulmann does not teach or allude to such subject matter. In fact, Ulmann does not refer to cryptography. In addition, Ulmann teaches a fixed, 32-bit instruction set, not a variable length instruction as is disclosed in the instant application.

With regard to Lynch, Applicant agrees that Lynch teaches the architecture for an x86-compatible microprocessor at a very broad level, including a load/store unit, as is cited by the Examiner in col 3, line 54 through col. 4, line 17. And Applicant wishes to refer the Examiner to the use of "floating point" in the instant disclosure, where it is discussed in the background. More specifically, Applicant refers to floating point *co-processors* which in former architectures where analogous to present day cryptographic *co-processors*, such as is alluded to by Qi. And, as stated earlier, prior to the advent of the present invention, there existed no microprocessor with an integral cryptographic unit. Hence, Lynch does not teach any mechanism or technique for translation of a cryptographic instruction into a sequence of micro instructions for execution by a cryptographic unit within a microprocessor.

Since none of the cited references teach the limitations noted above, alone, or in combination, Applicant respectfully requests that the rejection of claim 1 be withdrawn.

Claims 2-16 depend from claim 1 and add limitations over and above that subject matter which has been argued to be allowable over the prior art of record. Consequently, it is requested that the rejections of claims 2-16 be withdrawn.

With regard to independent claims 17 and 24, these claims contain substantially the same limitations as are found in claim 1, and which have been argued to be allowable over Qi, Ulmann, Lynch, or any combination of the three references. It is therefore requested that the rejections of clams 17 and 24 be withdrawn as well.

Claims 18-23 and 25-29 depend from claims 17 and 24, respectively, and add limitations over and above that subject matter which has been argued to be allowable over the prior art of record. Consequently, it is requested that the rejections of claims 18-23 and 25-29 be withdrawn.

RECEIVED
CENTRAL FAX CENTER
SEP 19 2007

CONCLUSIONS

Applicant believes this to be a complete response to all of the issues raised in the instant office action and further submits, in view of the amendments and arguments advanced above, that claims 1-29 are in condition for allowance. Reconsideration of the rejections is requested, and allowance of the claims is solicited.

Applicant also notes that any amendments made by way of this response, and the observations contained herein, are made solely for the purpose of expediting the patent application process in a manner consistent with the PTO's Patent business Goals (PBG), 65 Fed. Reg. 54603 (September 8, 2000), and are furthermore made without prejudice to Applicant under this or any other jurisdictions. It is moreover asserted that insofar as any subject matter might otherwise be regarded as having been abandoned or effectively disclaimed by virtue of amendments made herein and/or incorporated in attachments submitted with this response, Applicants wishes to reserve the right and hereby provides notice of intent to restore such subject matter and/or file a continuation application in respect thereof.

Applicant earnestly requests that the Examiner contact the undersigned practitioner by telephone if the Examiner has any questions or suggestions concerning this amendment, the application, or allowance of any claims thereof.

I hereby certify under 37 CFR 1.8 that this correspondence is being facsimile transmitted to the United States Patent and Trademark Office on the date of signature shown below.

Respectfully submitted,
HUFFMAN PATENT GROUP, LLC

/Richard K. Huffman/

By: _____

RICHARD K. HUFFMAN, P.E.
Registration No. 41,082
Tel: (719) 575-9998

09/19/2007

Date: _____